第三者の検証・妥当性確認による品質説明力の強化
～ソフトウェア品質監査制度（仮称）～

独立行政法人　情報処理推進機構　ソフトウェア・エンジニアリング・センター
統合系プロジェクト＆組込み系プロジェクト　サブリーダー

工学博士　田丸　喜一郎

ソフトウェア品質監査制度（仮称）検討の背景と経緯

第三者の検証・妥当性確認による品質説明力強化の必要性

品質説明に対する市場意識の変化

品質説明力の不足： 当事者企業の技術的主張だけでなく、第三者の裏付け（検証、妥当性確認）による品質説明への要求の増大

製品の利用者が感じる違和感

利用品質低下の懸念： 製品・システムの高度化・複雑化と利用者の多様化により、製品・システムと利用者との間のギャップが拡大

先端技術製品の潜在リスクへの不安

製品品質低下の懸念： 技術の急速な進歩により技術標準（規格）に基づく規格認証の対象範囲外となる領域が拡大

品質文化の異なる業界を跨るシステム

残存する潜在リスクの増加： 複数の業界を跨るシステムの拡大に伴い、全体システムとしての品質確認の精度が低下

第三者による検証・妥当性確認

事業者の技術的主張の妥当性を、監査機関が開発技術水準と利用技術水準を考慮して第三者の立場で評価し、技術に関する専門知識のない利用者にも理解できる形で情報提供する仕組み

（会計処理における会計監査と同等の役割）

IPA/SECでの活動経緯

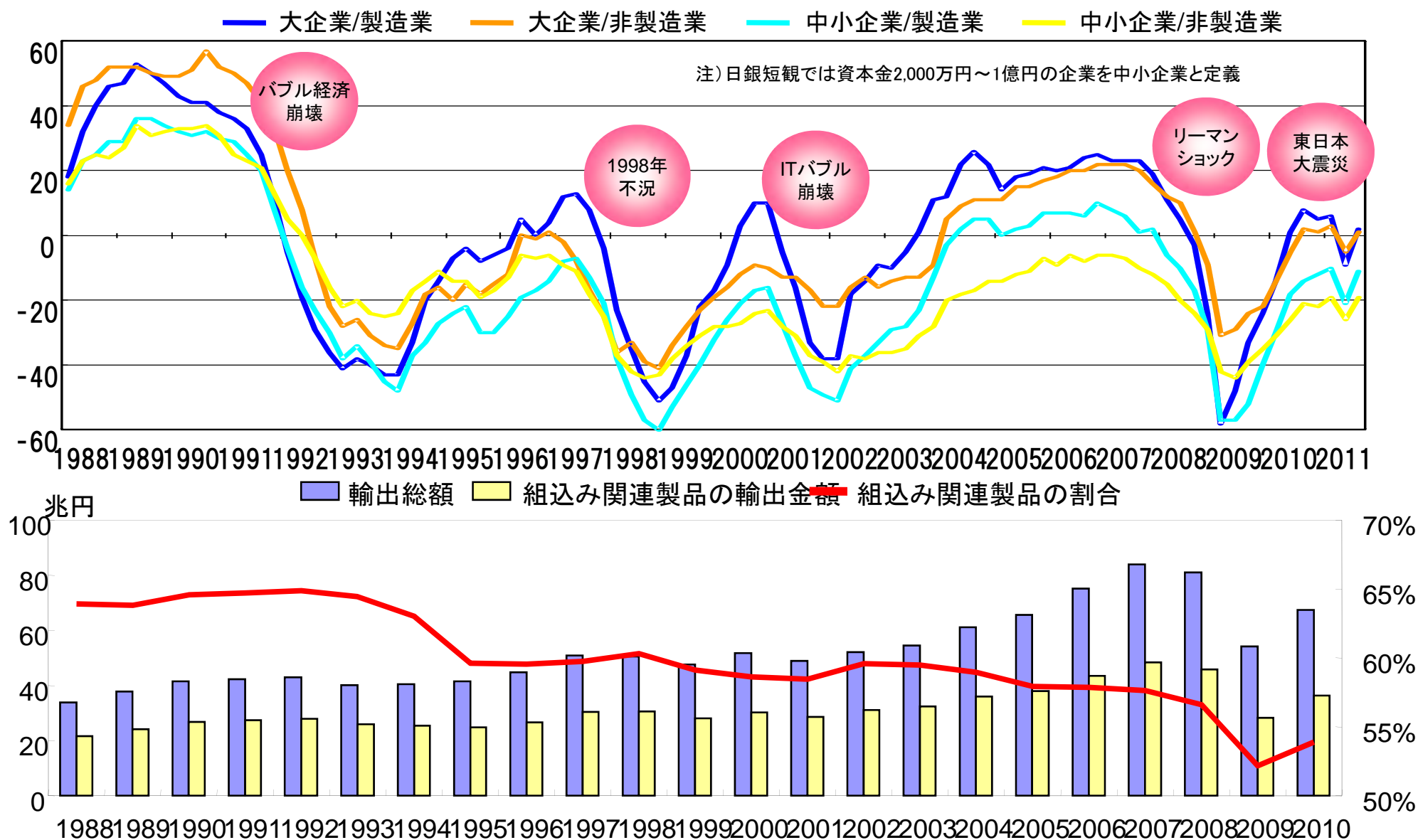
- 2010年3月：産構審情報システム・ソフトウェア小委員会にて第三者による検証・妥当性確認の枠組みの必要性が示される
- 2010年4月：IPA/SECの統合系プロジェクト内に検討チームを発足
- 2010年7月：調査活動開始
- 2010年11月：制度検討委員会発足（主査：名古屋大学高田教授）
- 2011年6月：中間報告

ソフトウェア品質監査制度（仮称）の狙いと効果
国民生活の安全・安心・快適の向上と我が国産業の国際競争力の強化

ソフトウェア品質監査制度（仮称）の狙い	ソフトウェア品質監査制度（仮称）の効果
企業の製品・システムに関する利用者や市場への品質説明力の強化	技術の専門家ではない利用者の安心感の向上
国際市場における日本製品・システムの品質に対する正当な評価の確立	我が国産業の国際競争力の維持・強化
産業界の枠を超えた品質の見える化による複数の産業界を跨り構成される高度なシステムの開発加速 （例：スマートコミュニティシステムなど）	国民生活の快適性・利便性の向上 新成長戦略分野における我が国産業の国際優位性の確保
製品・システムの本質的な品質向上	国民生活の安全性の確保

ご参考：米国の状況

- 2010年日本製自動車の制御システムに対する不具合の疑念が拡大。米国政府の要請で、NASAの独立検証・妥当性確認(IV&V)センターが第三者の立場で、制御システムの検証ならびに妥当性確認を実施。2011年2月、不具合が発見されなかったとの最終報告が公開。
- 当事者企業の主張だけでなく、第三者の主張がないと説明力が不充分との意識（会計処理における会計監査の必要性と同等の意識）。
- 国防省やNASAのシステムの調達、航空機分野、医療機器分野で類似した仕組みを運用している。

日銀短観(1988年3月～2011年9月:四半期毎)と輸出金額の推移(1988年～2010年暦年)

組込みシステム製品開発費と組込みソフトウェア開発費・開発費比率の推移

組込み製品開発費（1,000億円） 組込みソフトウェア開発費（1,000億円） 製品開発費に占める組込みソフトウェア開発費の割合

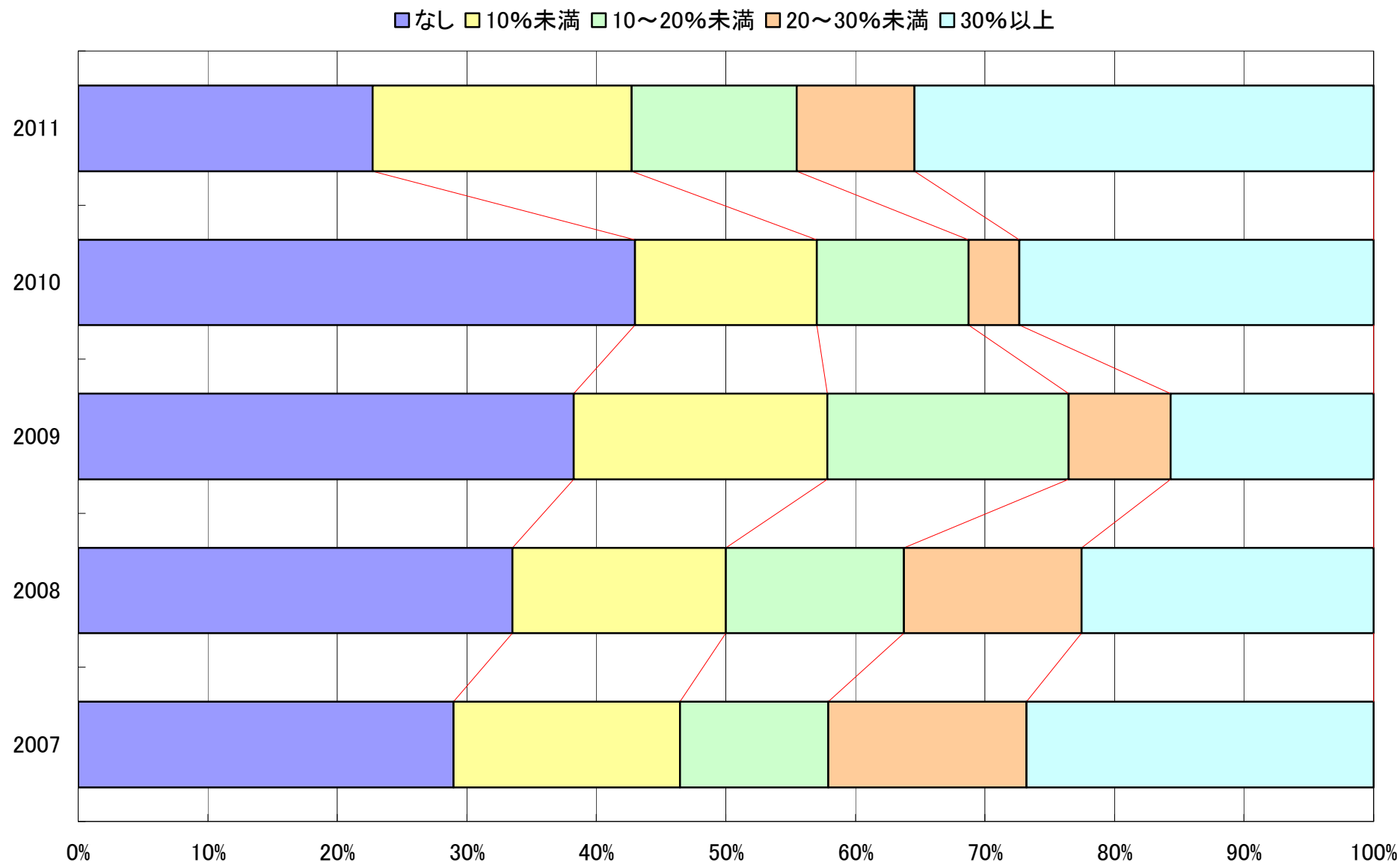
1000億円

組込みソフトウェア開発費の割合：49.6%
2004-20011年平均成長率(CAGR:Compound Annual Growth Rate)：5%

	組込み製品開発費（1,000億円）	組込みソフトウェア開発費（1,000億円）	製品開発費に占める組込みソフトウェア開発費の割合
2004年版	57.2	20.7	36.3%
2005年版	59.4	24.1	40.6%
2006年版	67.5	27.3	40.4%
2007年版	70.8	32.7	46.2%
2008年版	82.8	35.1	42.4%
2009年版	85.9	42.1	49.0%
2010年版	73.9	30.4	43.6%
2011年版	54.9	27.4	49.6%

左軸：0 20 40 60 80 100
右軸：0% 10% 20% 30% 40% 50% 60%

（社）日本機械工業連合会（平成21年度生産額実績統計）、組込みシステム産業の実態把握調査

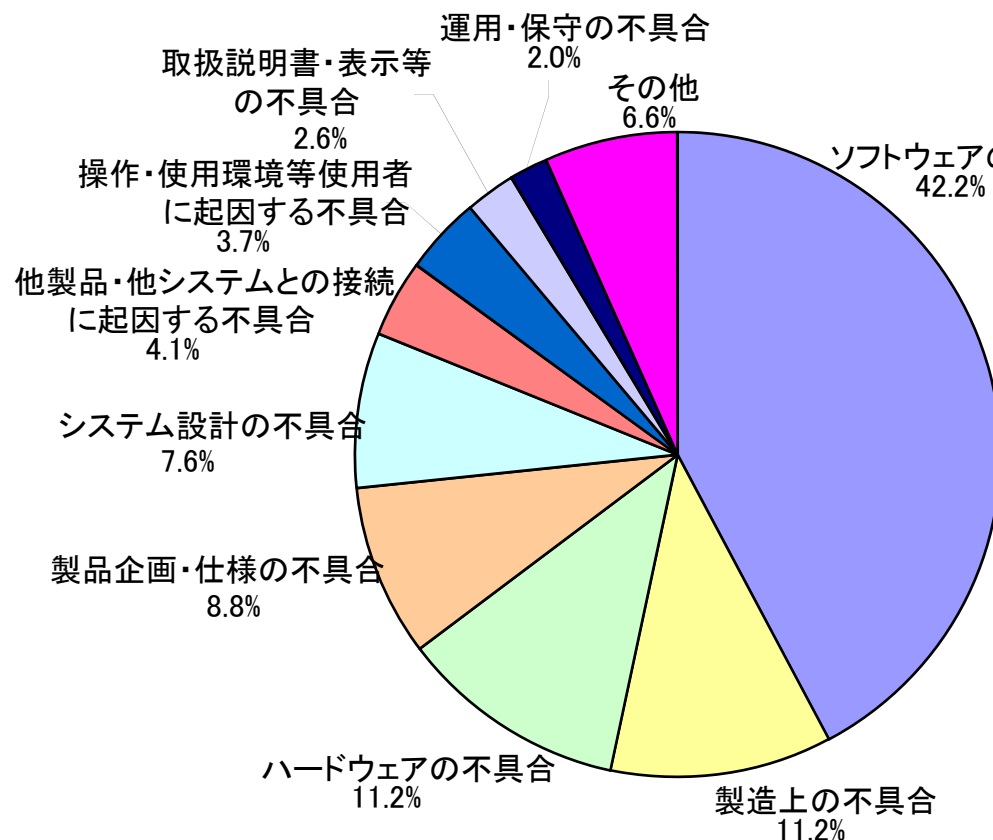
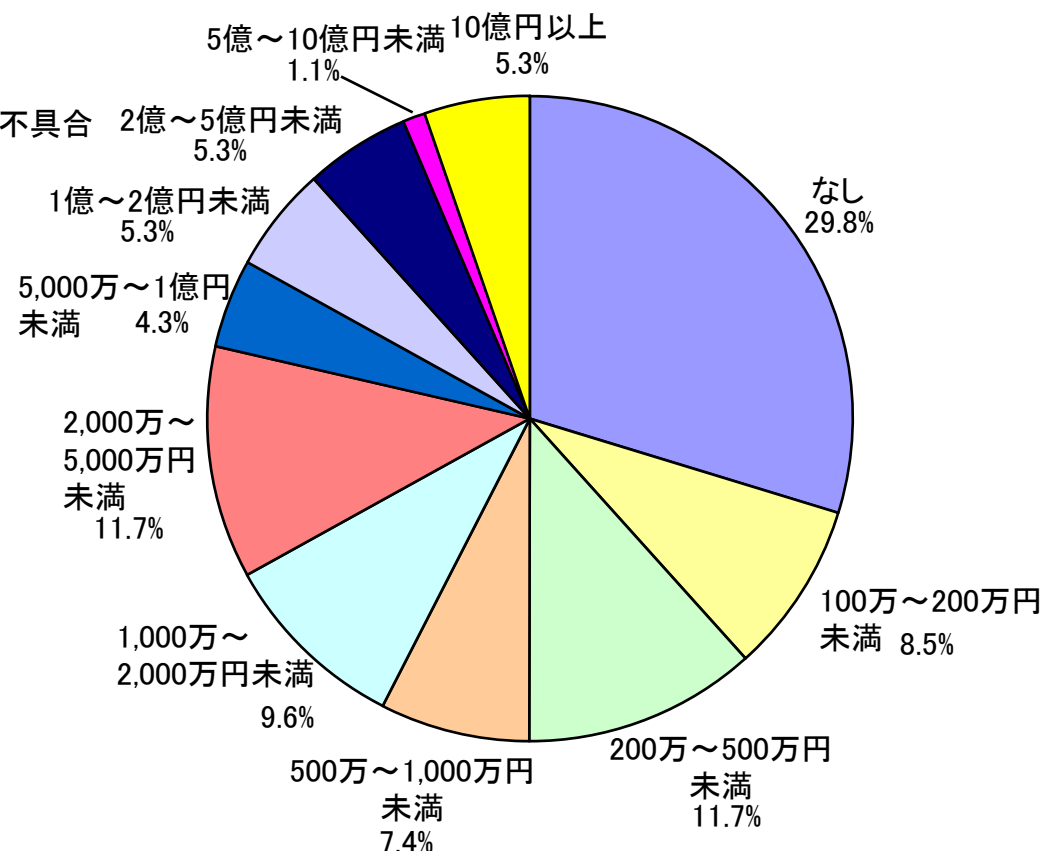
製品出荷後の不具合発生製品率の推移

出典:「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

製品出荷後の不具合の原因と「対策費＋損失」

不具合の原因（製品数ベース）

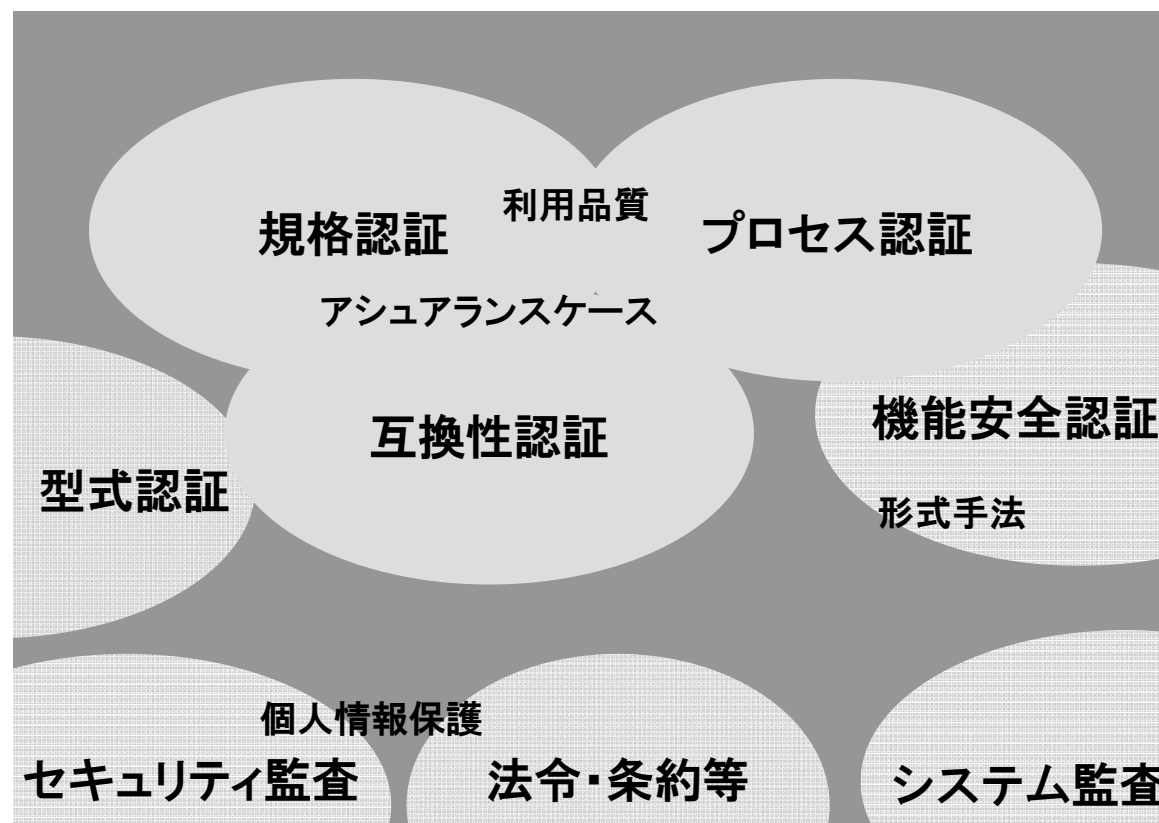
- ソフトウェアの不具合 42.2%
- 製造上の不具合 11.2%
- ハードウェアの不具合 11.2%
- 製品企画・仕様の不具合 8.8%
- システム設計の不具合 7.6%
- 他製品・他システムとの接続に起因する不具合 4.1%
- 操作・使用環境等使用者に起因する不具合 3.7%
- 取扱説明書・表示等の不具合 2.6%
- 運用・保守の不具合 2.0%
- その他 6.6%

「対策費＋損失」

- なし 29.8%
- 100万～200万円未満 8.5%
- 200万～500万円未満 11.7%
- 500万～1,000万円未満 7.4%
- 1,000万～2,000万円未満 9.6%
- 2,000万～5,000万円未満 11.7%
- 5,000万～1億円未満 4.3%
- 1億～2億円未満 5.3%
- 2億～5億円未満 5.3%
- 5億～10億円未満 1.1%
- 10億円以上 5.3%

出典：「経済産業省　平成22年度　組込みシステム産業の実態把握調査」

ソフトウェア品質監査制度(仮称)の特長

- 独立検証機関による検証と妥当性確認を包含
  - 事業者の主張を高度な専門技術を持った独立検証機関で再確認
- 利用情報や利用者情報に基づく利用品質の確認
  - すべての開発ライフサイクルでの利用情報、利用者情報の活用を確認
- 既存の認証制度や監査制度を補完
  - 既存の認証結果・監査結果を確認し、重複した監査を簡略化
- 開発ライフサイクルに合わせて開発と並行して監査を実施
  - 指摘事項への対応による手戻りが防止でき、出荷時期等への影響を最小化
- 機密情報の拡散リスクを低減できる内部審査官と外部審査官が連携
  - 外部審査官の管理下で内部審査官が機密情報を直接アクセスする監査業務を実施

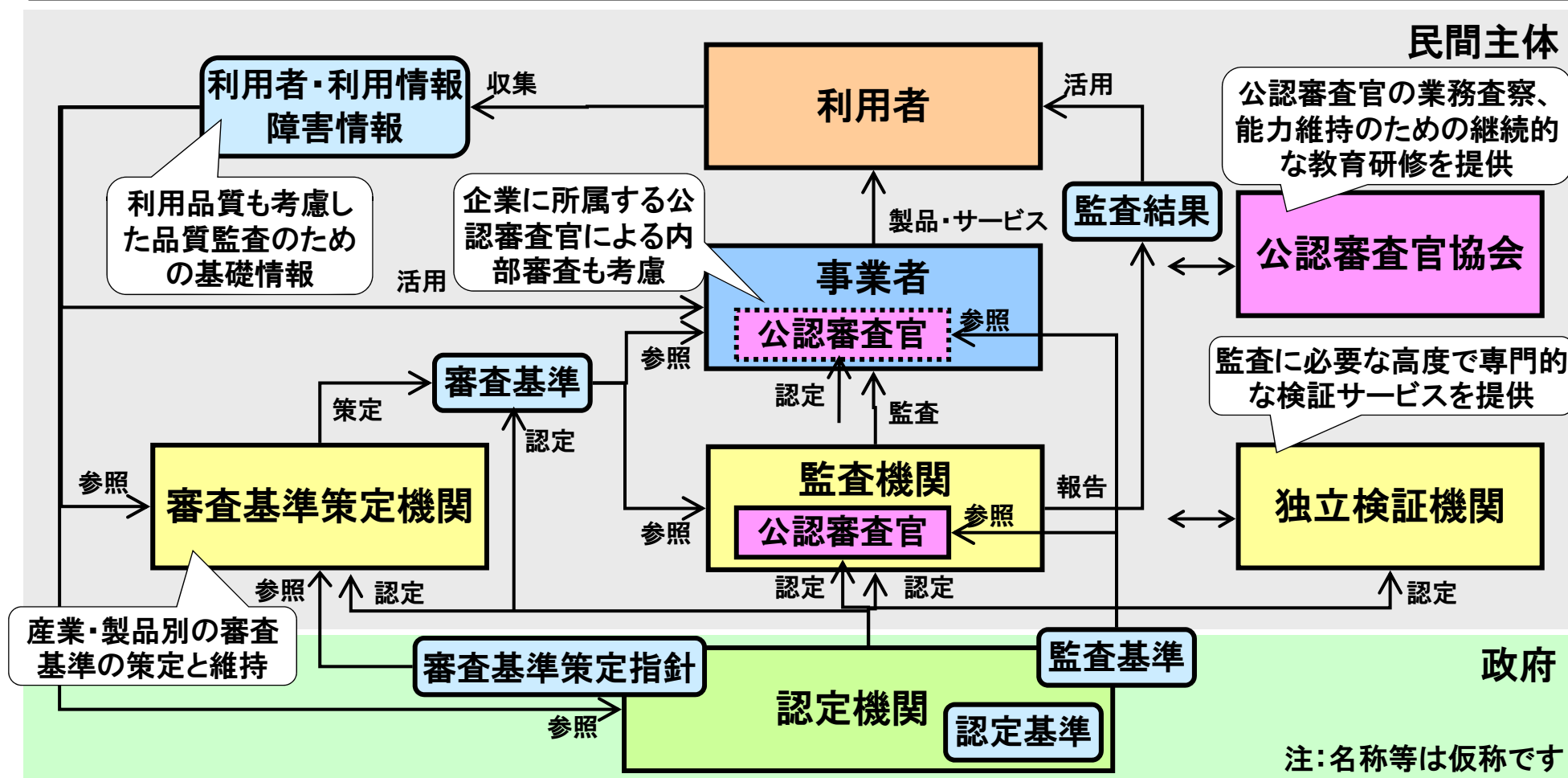
利用者・市場が期待する第三者による確認範囲

ソフトウェア品質監査制度(仮称)で監査する範囲
他の認証・監査の結果を確認する範囲

ソフトウェア品質監査制度（仮称）の枠組み
産業・製品分野別への対応と内部監査を考慮したフレームワーク

下記の要件を満たす「公認審査官」が、産業分野あるいは製品分野毎に定められた「審査基準」を基に、「監査基準」に従って監査業務を遂行し、「監査結果」を利用者にも理解できる形で情報提供する制度
- 要件1．専門性：情報の信頼性を保証できる専門知識と能力を有していること
- 要件2．独立性：監査対象の事業者・利用者から身分的・経済的・精神的に独立していること

民間主体

利用者・利用情報 障害情報
収集
利用者
活用
公認審査官の業務査察、能力維持のための継続的な教育研修を提供
利用品質も考慮した品質監査のための基礎情報
企業に所属する公認審査官による内部審査も考慮
製品・サービス
監査結果
公認審査官協会
活用
事業者
公認審査官
参照
参照
審査基準
策定
認定
監査
監査に必要な高度で専門的な検証サービスを提供
認定
参照
審査基準策定機関
監査機関
公認審査官
報告
参照
参照
独立検証機関
参照
認定
認定
認定
認定
産業・製品別の審査基準の策定と維持
審査基準策定指針
監査基準
政府
認定機関
認定基準
参照

注：名称等は仮称です

品質問題に起因する影響の度合いに応じて監査内容を定義
要求される品質説明力と監査コストとのバランス

利用者・国民への影響度と産業界・経済への影響度によりレベル分け（監査レベル）し、監査レベル毎に監査内容を定義する。

監査レベル

産業・経済影響レベル ＼ 利用者・国民影響レベル	0	1	2	3	4
4	4	4	4	4	4
3	3	3	3	3	4
2	2	2	2	3	4
1	1	1	2	3	4
0	0	1	2	3	4

監査レベルに対応した監査内容

監査レベル	監査する審査項目	監査方法	独立検証
4	全項目	網羅監査（全件監査）	必須
3	重要項目	網羅監査（全件監査）	必須
	その他の全項目	抜取監査（サンプル監査）	任意
2	全項目	抜取監査（サンプル監査）	任意
1	重要項目	抜取監査（サンプル監査）	任意
0	非対象	非対象	非対象

産業・経済影響レベル

レベル	影響の範囲
4	我が国の産業への広範囲な影響
3	当該産業に限定された影響 当該企業以外の同一・類似産業のへの影響
2	当該企業に限定された影響 当該製品・サービス以外の他事業への影響
1	当該製品・サービス事業に限定された影響
0	影響はない／ほとんど影響はない

利用者・国民影響レベル

レベル	影響の範囲・程度
4	当該利用者ならびに当該利用者以外への重大な影響（代替手段による影響軽減が困難な影響） 国民への広範囲で重大な影響
3	当該利用者への重大な影響に加え、当該利用者以外への軽微な影響（代替手段による影響軽減が容易な影響）
2	当該利用者に限定された重大な影響
1	当該利用者に限定された軽微な影響
0	影響はない／ほとんど影響はない

内部監査を適用する場合の外部審査官と内部審査官の役割

監査計画の立案：

・内部審査官が審査対象組織と協議し、開発情報の機密性を評価し、内部監査での実施と外部監査での実施に峻別して、監査計画案を策定する
・監査計画案の外部審査官の合意を得て監査計画を確定する

監査の実施：

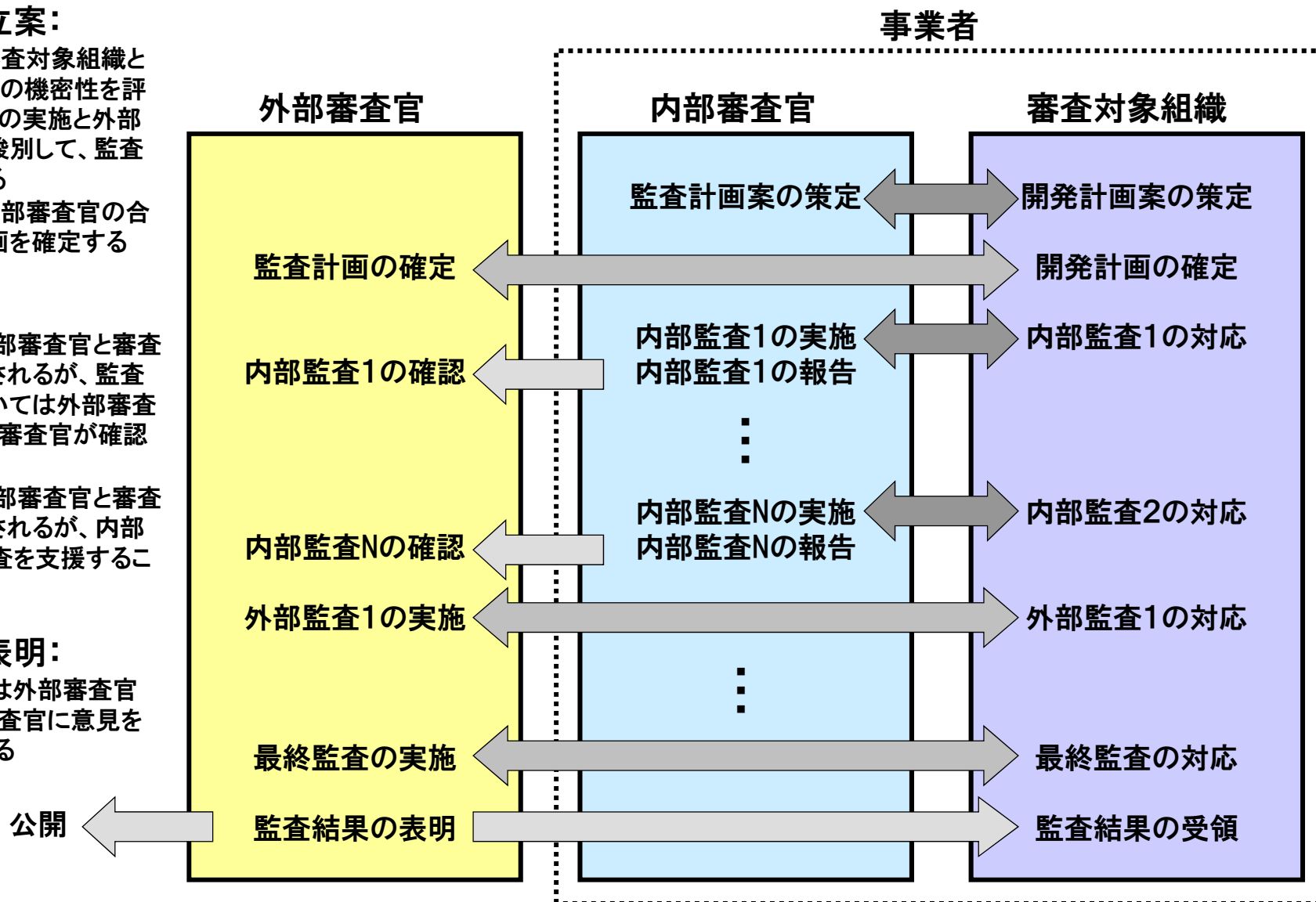
・内部監査は、内部審査官と審査対象組織で実施されるが、監査の実施状況については外部審査官に報告し、外部審査官が確認する
・外部監査は、外部審査官と審査対象組織で実施されるが、内部審査官は外部監査を支援することができる

監査結果の表明：

監査結果の表明は外部審査官が行うが、内部審査官に意見を求めることができる

事業者

外部審査官	内部審査官	審査対象組織
	監査計画案の策定	開発計画案の策定
監査計画の確定		開発計画の確定
内部監査1の確認	内部監査1の実施 内部監査1の報告	内部監査1の対応
	：	
内部監査Nの確認	内部監査Nの実施 内部監査Nの報告	内部監査2の対応
外部監査1の実施		外部監査1の対応
	：	
最終監査の実施		最終監査の対応
監査結果の表明		監査結果の受領

公開 ← 監査結果の表明

独立検証機関を有する企業の他事業との関係

- 事業者向け受託開発サービス事業、事業者向けIV&Vサービス事業、その他の事業を字実施する企業等も、それらの事業と独立性を担保することで独立検証機関として認定
  - 独立した意思決定機構（独立した事業責任者の設置等）、独立した予算、独立性に関する内部監査など
- 独立検証機関としての業務査察、能力維持のための継続的な教育研修については関連の業界団体の実施を想定

民間主体

利用者

製品・サービス

事業者

公認審査官

認定

監査

監査機関

公認審査官

認定

認定

企業

下記以外のその他の事業

事業者向け受託開発サービス事業

事業者向けIV&Vサービス事業

監査機関向けIV&Vサービス事業

認定

独立検証機関として事業を認定された企業

独立検証機関としての業務査察、能力維持のための継続的な教育研修を提供

業界団体

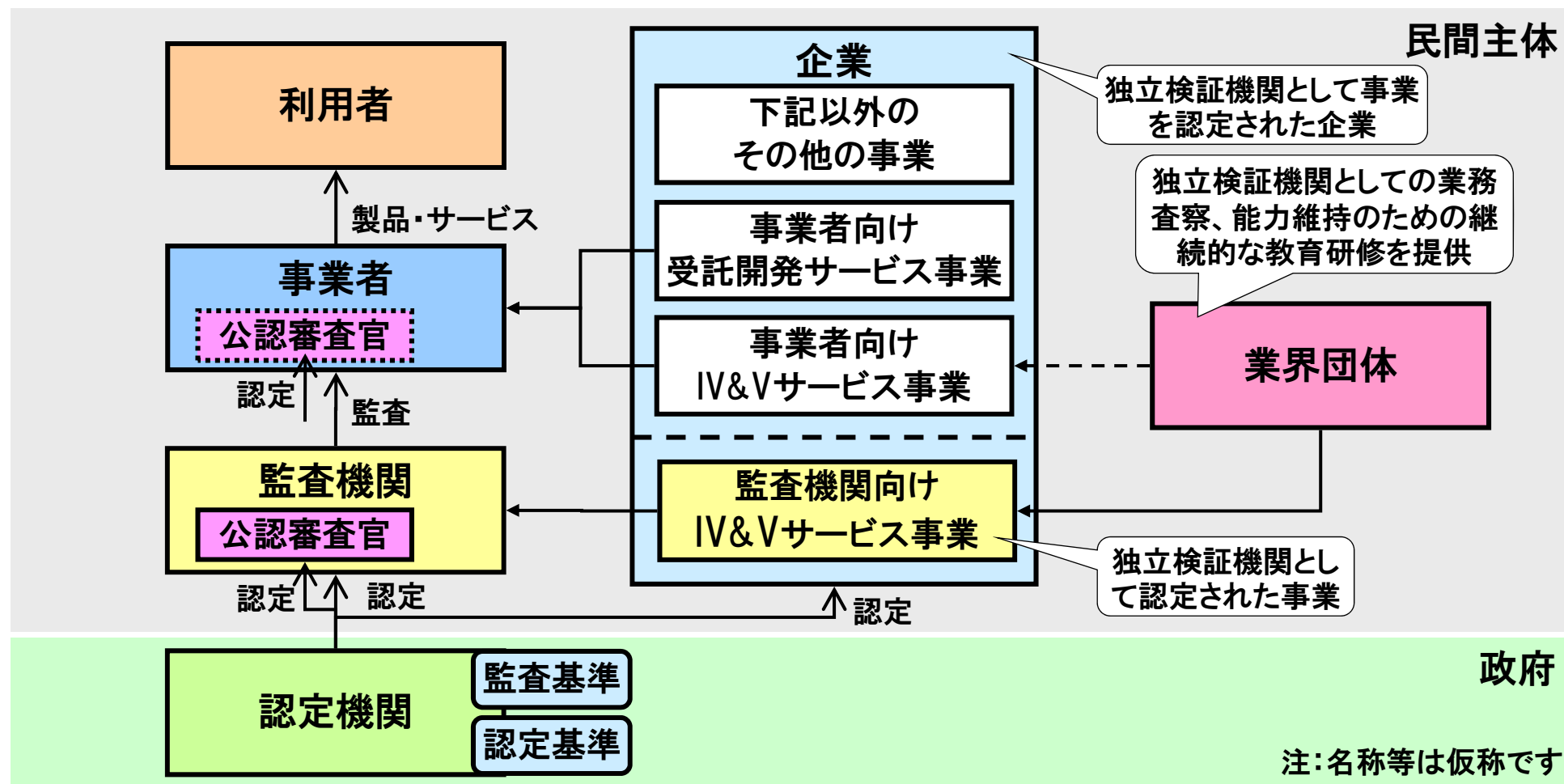
独立検証機関として認定された事業

政府

認定機関

監査基準

認定基準

注：名称等は仮称です

派生開発、系列開発、差分開発等における監査の取り扱い

既開発の改変部分：
・同一監査レベル以上で監査済みの場合は、監査結果を確認し、改変部分とその影響範囲に絞った監査を実施する
・上記以外の場合は、通常の監査を実施する

既開発部分（改変無し）：
・同一監査レベル以上で監査済みの場合は、監査結果を確認し、監査を省略できる
・上記以外の場合は、通常の監査を実施する

新規開発部分：
・監査レベルに応じた通常の監査を実施する（再利用を予定している場合は、それらの利用を考慮して監査レベルを決定することが望ましい）

新規開発部分
既開発の改変部分
既開発部分
市販ソフトウェアの導入部分
オープンソースソフトウェアの導入部分
システム統合部分

市販ソフトウェアの導入部分：
・同一監査レベル以上で監査済みの場合は、監査結果を確認し、監査を省略できる
・上記以外の場合は、採用を推奨しないが、あえて採用する場合は、提供元に監査の実施を依頼するか、監査への協力を依頼する（監査レベルが低くなる使用方法も考慮）

オープンソースソフトウェアの導入部分：
・市販ソフトウェアと同等に監査済みソフトウェアとして導入した場合（ディストリビュータ経由等）は、同一監査レベル以上で監査済みの場合は、監査結果を確認し、監査を省略できる
・上記以外の場合は、ソースコードからの検証を含めた監査を実施する

システム統合部分：
・新規開発部分以外のすべての部分について、それらの採用ならびに利用の妥当性に関する監査を実施する（プラットフォームやハードウェアの相違などによる影響等を考慮）

ソフトウェア品質監査を効率的に実施できる開発プロセス（要件ベース）

階層化されるソフトウェア開発工程を要件で受渡し

要求

システム要件定義

要求分析

設計結果

システム要件

サブシステム要件定義

システムアーキテクチャ設計

設計結果

サブシステム要件

コンポーネント要件定義

サブシステムアーキテクチャ設計

設計結果

コンポーネント要件

コンポーネント実装

コンポーネント設計／実装／デバッグ

コンポーネント

サブシステム結合テスト

サブシステム

システム結合テスト

システム

運用テスト

上下の要件間の確認が容易

暗黙知から形式知化

従来、要件は暗黙知であったが、
本プロセスでは、
要件を形式知とする

それぞれ要件があるため、要件と出来たものの通り振る舞うかの検証が容易

要件と仕様の確認が容易

外部に発注する際にも要件でやりとりした方が良い
（要件を実現する仕様は数多くあるため、要件を明確に定義しておく必要がある）

要件ベース開発プロセスの各要件定義工程のタスクモデル

外部設計、内部設計(構造設計)、下位要件の検証・妥当性確認を工程内で閉じて実施可能

上位要件

××要件定義

レビュー

レビュー結果

外部設計(仕様設計)

外部設計書

外部設計検証

外部設計検証結果

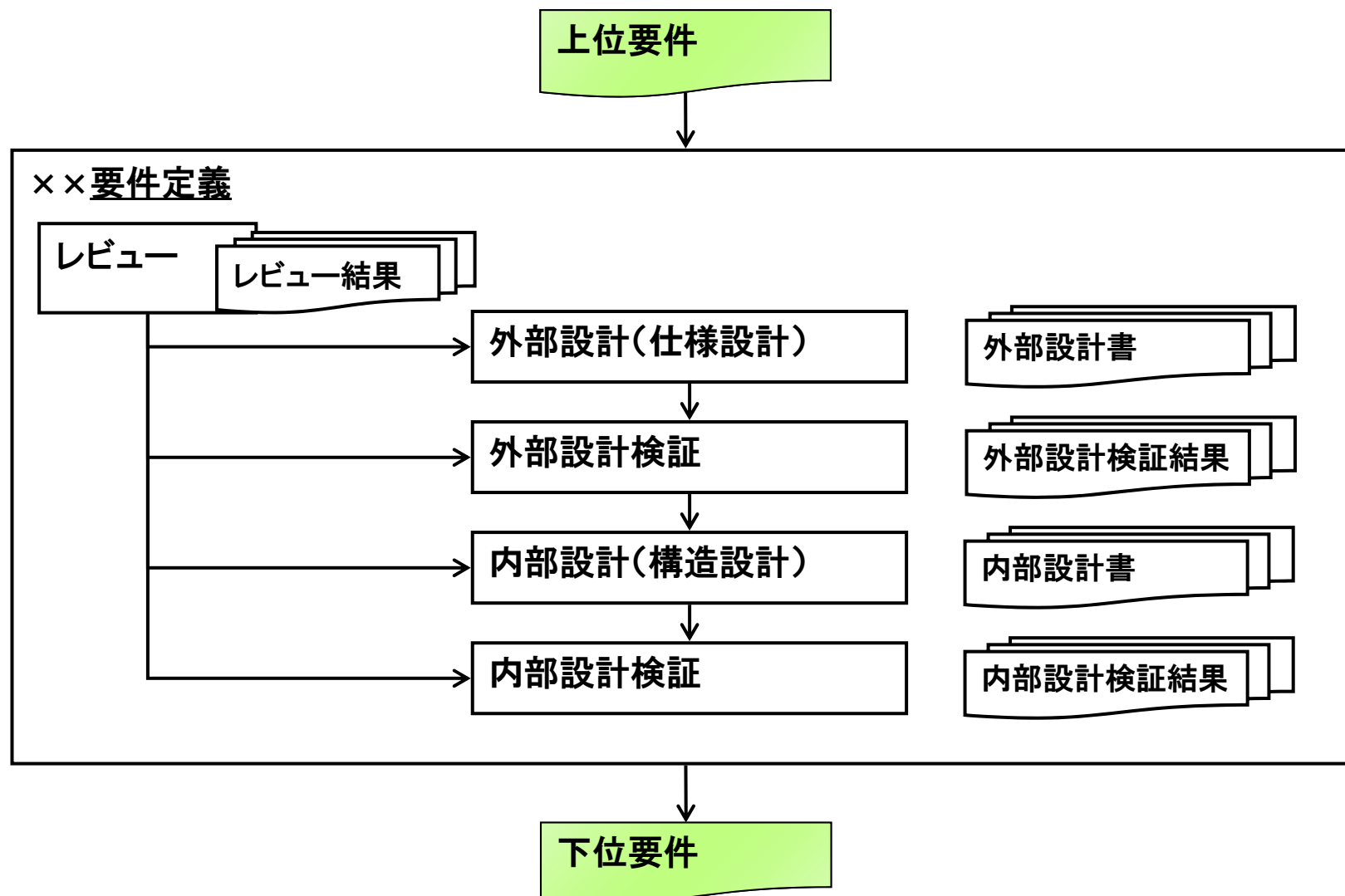
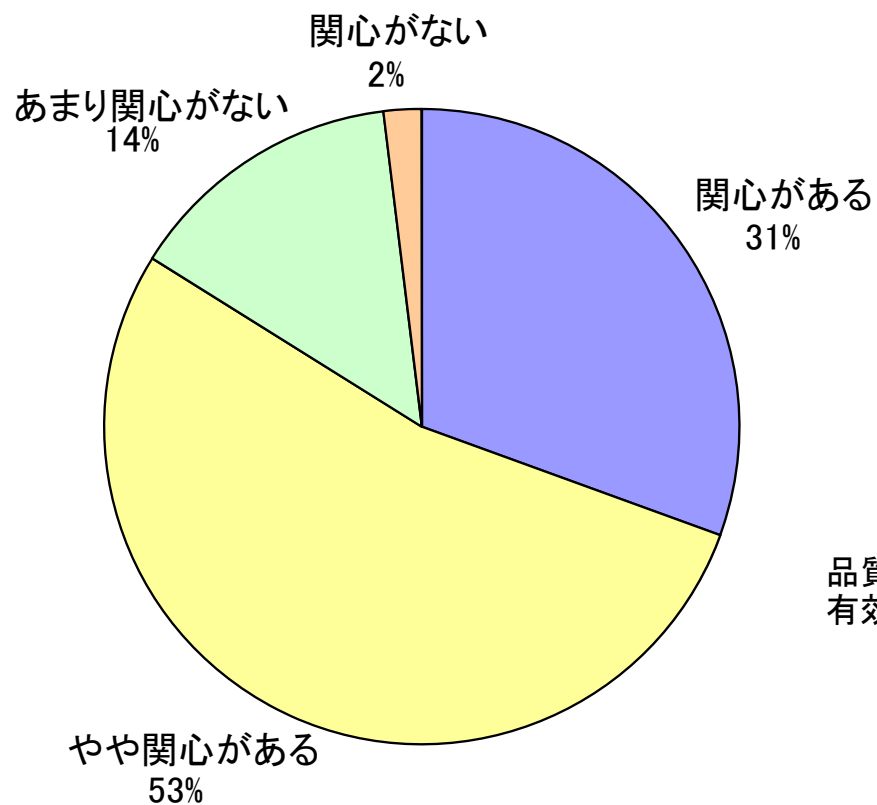
内部設計(構造設計)

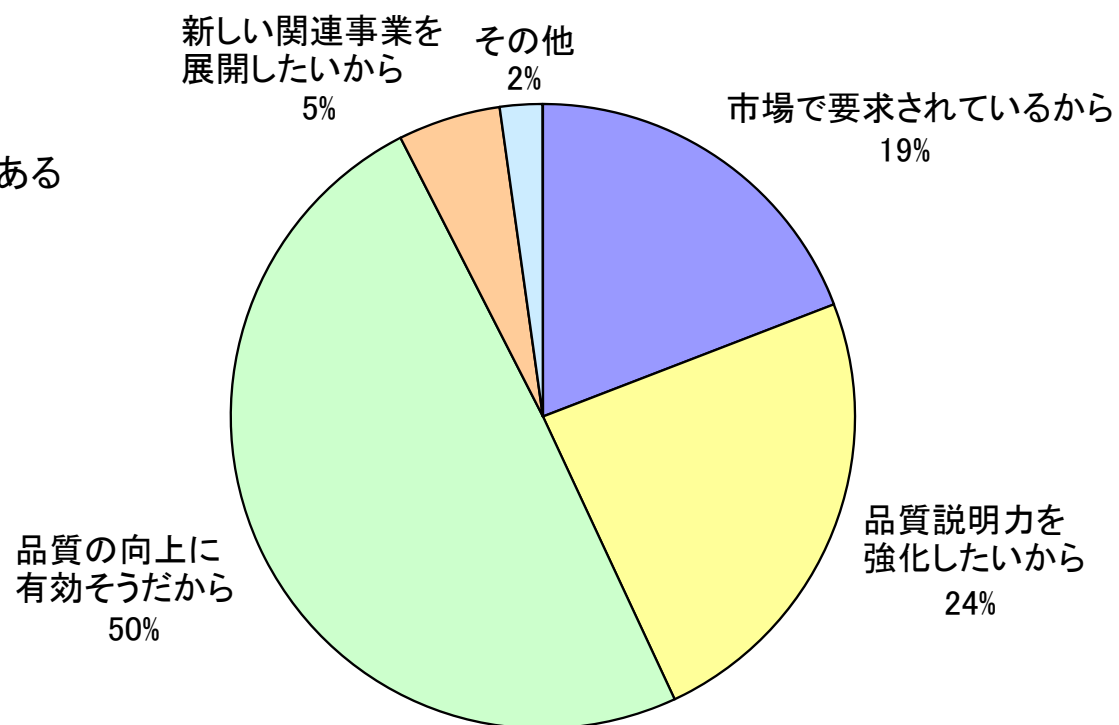
内部設計書

内部設計検証

内部設計検証結果

下位要件

ESEC(2011年5月)のIPA/SECブース来場者へのアンケート結果

品質監査制度(仮称)に関心がありますか？
(回答数:2154名)

どのような観点で関心がありますか？
(回答数:1985名)

ET-West(2011年6月)のSECセミナー聴講者のアンケート結果（回答数:93名）

「ソフトウェア品質監査制度(仮称)に関心があるか？

どのような観点で関心があるか？

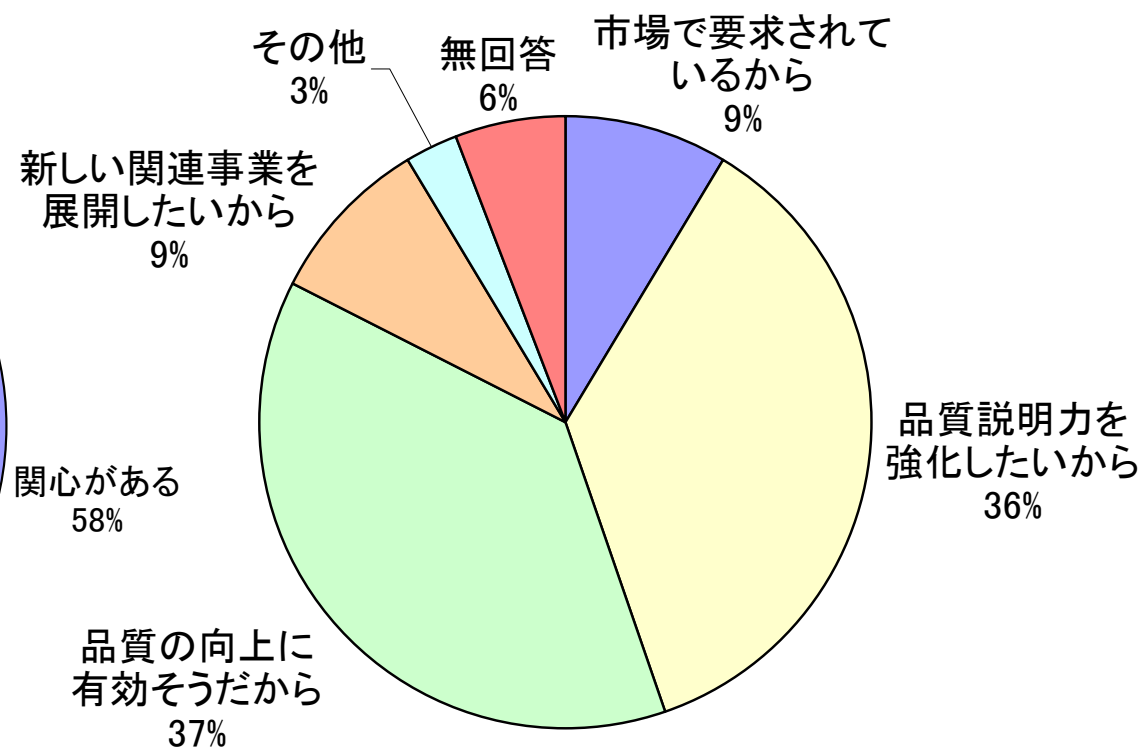
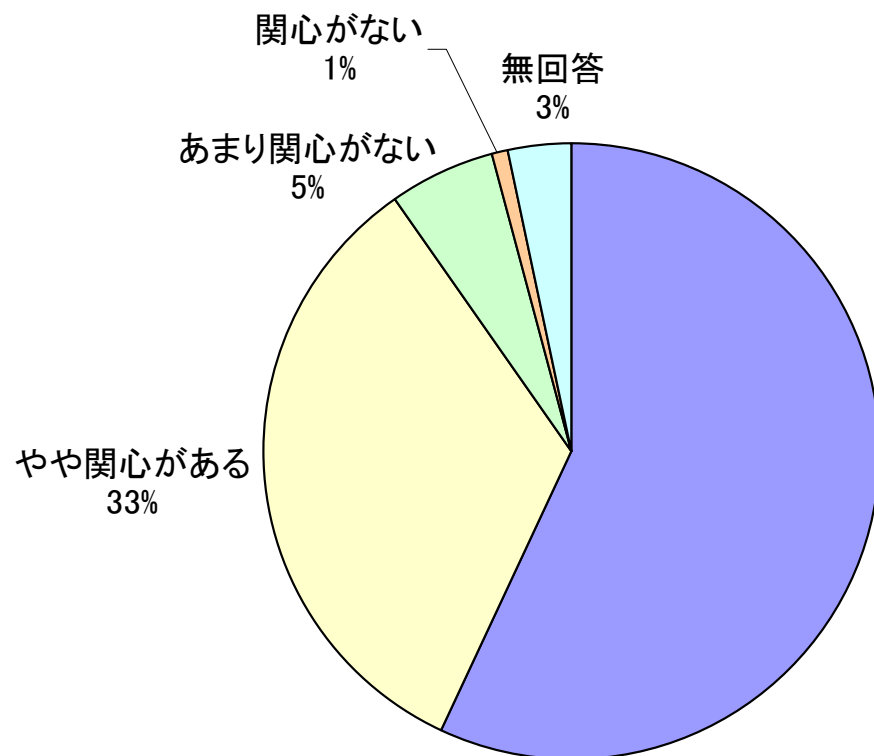
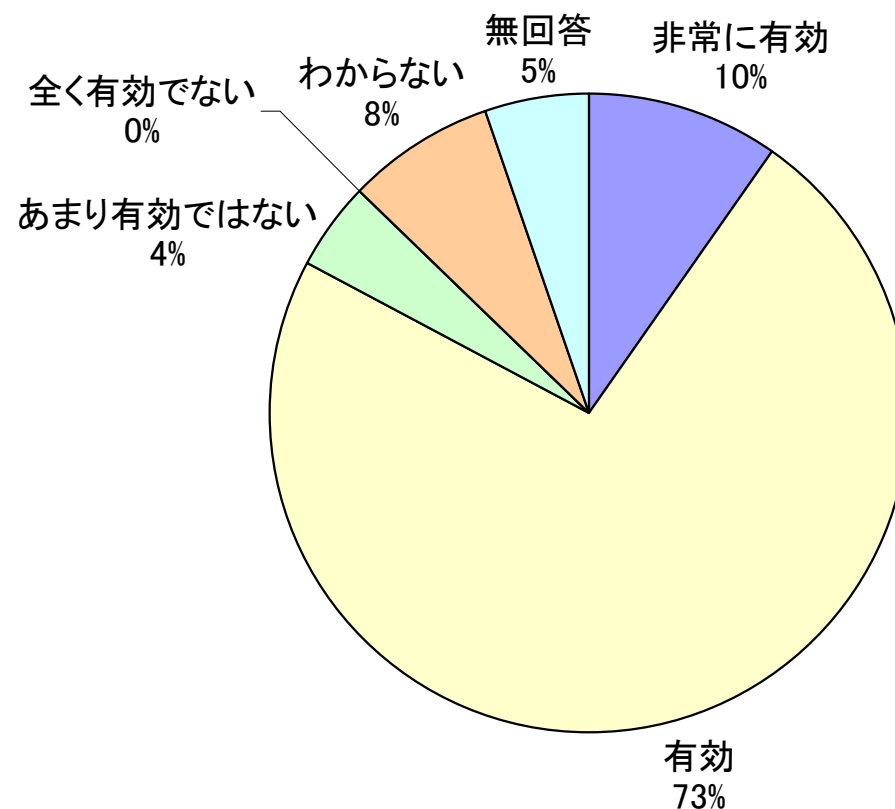
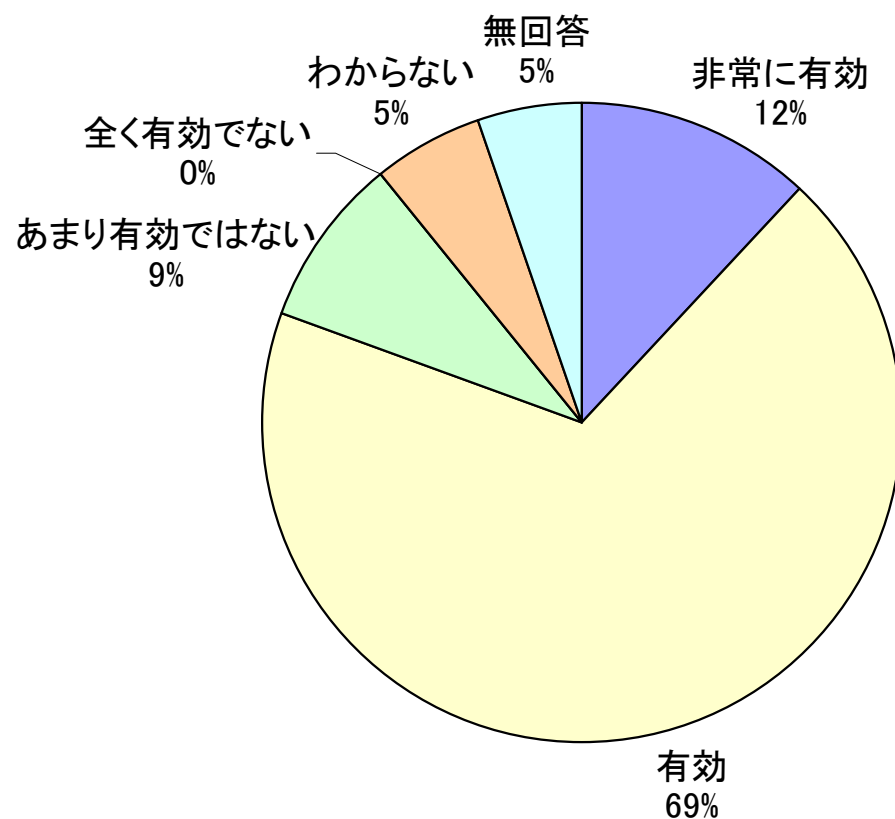
ET-West(2011年6月)のSECセミナー聴講者のアンケート結果（回答数:93名）

「利用者」にとって本制度は有効と思われるか？

回答	割合
非常に有効	12%
有効	69%
あまり有効ではない	9%
全く有効でない	0%
わからない	5%
無回答	5%

「事業者}にとって本制度は有効と思われるか？

回答	割合
非常に有効	10%
有効	73%
あまり有効ではない	4%
全く有効でない	0%
わからない	8%
無回答	5%

ET-West(2011年6月)のSECセミナー聴講者のアンケート結果 (回答数:93名)

第三者による検証・妥当性確認を実施しているか？

品質説明力強化のためにどれくらい投資すべきか？ 開発費を基準とした割合(%)

ご清聴ありがとうございました